PRACTICAL: 2

AIM:

You are a penetration tester hired by a small corporate company to assess the security of their internal network. The network consists of several devices, including servers, routers, workstations, and IoT devices. The company has provided a range of IP addresses for you to scan, but they want you to assess the vulnerabilities and misconfigurations on their internal systems using Nmap.
objectives:
1. Map the network: Discover which devices are active on the network.
2. Identify open ports and services: Check which ports are open and identify the services running on them.
3. Identify OS and versions: Detect the operating systems and their versions running on different hosts.
4. Perform a vulnerability scan: Check for common vulnerabilities and exposures.

THEORY:

Network Scanning: A technique used to discover devices, services, and open ports in a network, essential for assessing security.
Nmap (Network Mapper): A powerful open-source tool for network discovery, service identification, OS detection, and vulnerability assessment.
Port Scanning: Identifies open ports and the services running on them, highlighting potential entry points for attackers.
OS Detection: Determines the operating system and version on target hosts to assess their compatibility and security posture.

CODE:

1. Mapping and Scanning the Network

```
nmap -sn 192.168.57.174
```

-sn: Performs a ping scan to identify live hosts without scanning for open ports.

2. Identify the open ports and services

```
nmap -sS -sV 192.168.57.174
```

-sV: Enables version detection to identify services running on open ports.

3. Identify OS and versions

```
nmap -O 192.168.57.174
```

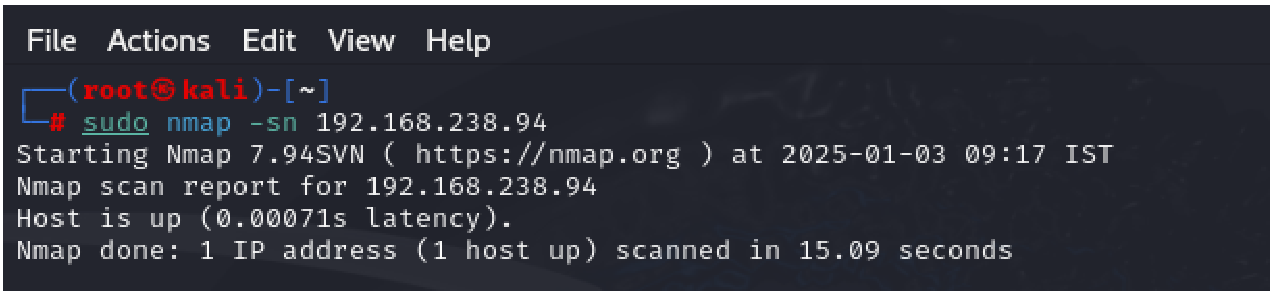
-O: Enables operating system detection.

4. Perform vulnerability scan

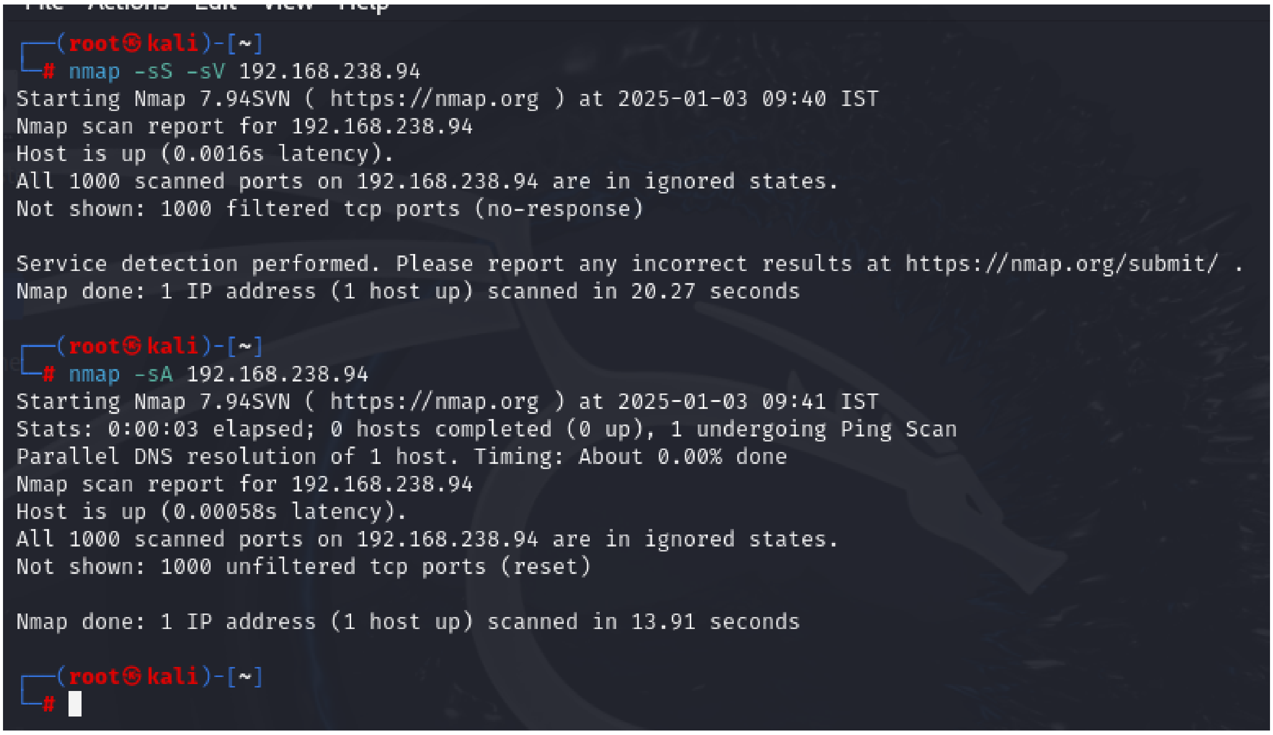
```
nmap --script vuln 192.168.57.174
```

--script vuln: Runs Nmap's built-in vulnerability scripts to check for known vulnerabilities.

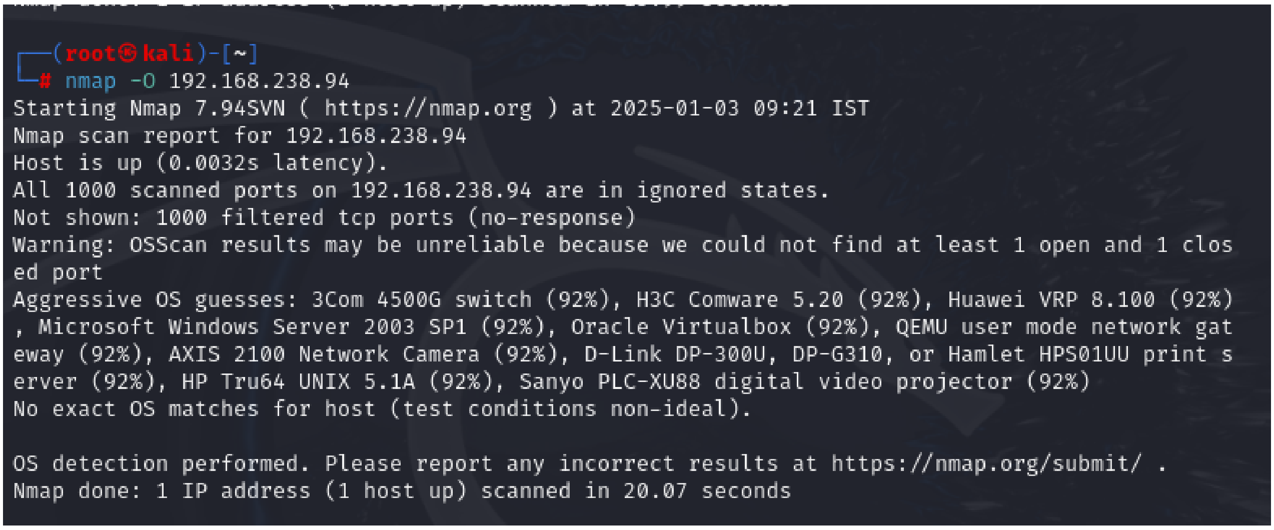
OUTPUT:



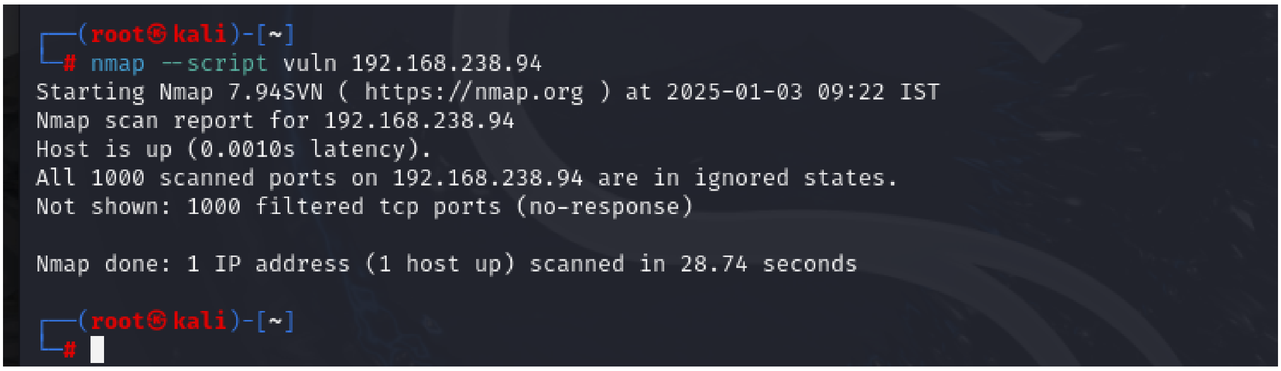
```
┌──(root㉿kali)-[~]
└─# sudo nmap -sn 192.168.238.94
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 09:17 IST
Nmap scan report for 192.168.238.94
Host is up (0.00071s latency).
Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -sS -sV 192.168.238.94
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 09:40 IST
Nmap scan report for 192.168.238.94
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.238.94 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.27 seconds

┌──(root㉿kali)-[~]
└─# nmap -sA 192.168.238.94
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 09:41 IST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.238.94
Host is up (0.00058s latency).
All 1000 scanned ports on 192.168.238.94 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.91 seconds

┌──(root㉿kali)-[~]
└─# 
```



```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.238.94
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 09:21 IST
Nmap scan report for 192.168.238.94
Host is up (0.0032s latency).
All 1000 scanned ports on 192.168.238.94 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clos
ed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%)
, Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox (92%), QEMU user mode network gat
eway (92%), AXIS 2100 Network Camera (92%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print s
erver (92%), HP Tru64 UNIX 5.1A (92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.07 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap --script vuln 192.168.238.94
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 09:22 IST
Nmap scan report for 192.168.238.94
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.238.94 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 28.74 seconds

┌──(root㉿kali)-[~]
└─# 
```

LATEST APPLICATIONS:

Network Mapping and Inventory: Nmap creates detailed maps of computer networks, detects live hosts, and helps manage network inventories.

OS and Port Scanning: Identifies operating systems, open ports, and running services on local and remote systems for security assessments.

Vulnerability and Zero-Day Detection: Uses Nmap scripts to identify vulnerabilities, including zero-day threats, and enhance proactive security measures.

Web Application Testing: Assesses vulnerabilities in web servers and complements tools like Burp Suite for comprehensive analysis.

LEARNING OUTCOME:

From this practical, I learned about network scanning and vulnerability assessment. I explored how to use Nmap to discover active devices and services on a network, identify open ports, detect operating systems running on different hosts, and perform basic vulnerability scans to highlight potential security risks.

REFERENCES:

1. Nmap Guide: https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/
2. Nmap: https://nmap.org/book/man.html
3. Nmap Official: https://nmap.org/docs.html